# Survivability and Information Assurance Curriculum Lab Overview

*Survivability and Information Assurance (SIA) Curriculum Development Team*
*CERT® Program*
*Software Engineering Institute*
*Carnegie Mellon University*
*Pittsburgh, PA*

## Introduction

All of the courses in the SIA Curriculum contain exercises, guided tours, and demonstrations that make use of computer systems. These computer systems are assumed to be located and networked together, preferably in a single room. For the specifics of how to set up and configure these computer systems for each course, see the Guided Tours entitled *Building the Lab Computer Systems for "Principles of Survivability and Information Assurance"*, *Building the Lab Computer Systems for "Information Assurance Networking Fundamentals"*, and *Building the Lab Computer Systems for "Sustaining, Improving, and Building Survivable Functional Units (SFUs)"*. This document describes the general lab hardware and software configuration, as well as, any ancillary equipment needed by each course.

## Hardware

There are two types of computer systems in the lab: the instructor computer system and the student computer systems. There should be one instructor computer system and a minimum of fourteen student computer systems. It is strongly recommended that each student have his or her own computer system so they can do the exercises individually. The fourteen student computer systems minimum comes from the number of computer systems designed into the enterprise in "Sustaining, Improving, and Building Survivable Functional Units (SFUs)." [Note carefully that the Software Engineering Institute has no responsibility to actually produce this enterprise lab.]

Each of these computer systems is a workstation that has a graphical display, a keyboard, and a mouse. The student computer systems should have a 3Ghz CPU, 2 GB of RAM, 80 GB of hard disk, a floppy disk drive, a CD/DVD reader, and a 10/100 Ethernet network interface card. The instructor computer system is identical to the student computer systems except that it should have 160 GB of hard disk and a CD/DVD recorder.

The lab should also have a printer, preferably a network-attached laser printer. During exercises, students need to print their work to turn in for grading. More than one printer will likely reduce bottlenecks and is recommended where possible.

## Software

The student and instructor computer systems run Red Hat LINUX Version 9 which is freely available[1] from http://www.redhat.com/. The patches to this version are also available at that site[2].

The courseware also uses many other public domain software packages that are also freely available[3]. The Guided Tours for each course identify where to retrieve these packages and how

® CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
[1] As of October 2005
[2] As of October 2005

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **NOV 2005** | | **00-00-2005 to 00-00-2005** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Survivability and Information Assurance Curriculum Lab Overview** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **8** | |

to install and configure them. The institution is responsible for retrieving all of the software packages[4] for the courses in the SIA Curriculum.

The student and instructor computer systems also use VMware Workstation version 4.5.2 for LINUX. This is a commercial product that is available from http://www.vmware.com/. The institution should purchase one license per computer system. The Guided Tours again describe how to install VMware Workstation version 4.5.2 for LINUX. There are many guided tours, exercises, and demonstrations where the students are shown how to use many of the features of VMware Workstation for LINUX.

## Configuration Management

All of the computer systems in all of the courses should be managed so that configure, repair, and rebuild activities can be centralized and can be carried out from the instructor computer system. While the selection of the specific technique is the responsibility of the institution, packages such as *kickstart*, which is provided by Red Hat LINUX as part of the Version 9 distribution, is a technique that should be considered. An institution's Information Technology organization may already have methods for managing LINUX -based clusters that may be adaptable for the labs described in this document.

Specifically, there should be two features engineered into the lab. They are:

1. File sharing where the instructor computer system is the file server and the student computer systems are the clients of that file server. There are many files that need to be available to the student computer systems that need not reside on the student computer systems. These can be provided by the instructor computer system using any of the available file sharing schemes. One provided by Red Hat LINUX Version 9 is Sun Microsystems's NFS. NFS has all of the necessary functionality (file sharing and access control) needed throughout the SIA Curriculum.
2. Remote command execution where the set of properly identified and authenticated users on the instructor computer system can remotely execute commands on any of the student computer systems. Again, while there are many schemes available, one provided by Red Hat LINUX Version 9 is SSH, the Secure Shell. SSH has all of the necessary functionally (strong authentication, remote command execution, and file transfer) that is needed throughout the SIA Curriculum.

## User Identity and Privileges

With respect to student user identity, it is suggested that all students use the same account on all of the student computer systems. Create a single user ID, `sia` , and a single group ID, also `sia,` that all students use.

Students will need to do some operations on the student computer systems with root privileges. There are two ways to achieve this. They are:

1. Give all of the students the root password. Once they've got that password, they can do all that they need to do and (unfortunately) all that they want to do.
2. Give specific privileges that are accessed through the **sudo**(8) program. In this way, students can gain access to what they need and nothing more. This method is used on the instructor computer system to build VMware-based guest computer systems as needed.

---

[3] As of October 2005

[4] This assumes the licensing/use conditions of the software packages allow this.

 

## Internet Connectivity

The lab need not be connected to the Internet. While there are benefits to the students to have Internet access while they are doing exercises, it is not a requirement. However, since all of the software used throughout the SIA Curriculum is available through the Internet, the instructor or those responsible for the setup and maintenance of the lab will need Internet connectivity at some point in time. Should the lab not be connected to the Internet, the recommended way to transfer the needed software packages[5] is through either burning DVDs or an external disk drive, for example a USB-connected external hard disk. Packages[6] are retrieved from sites on the Internet and then transferred to the lab through DVDs or the external hard disk drive. Note that the external disk drive does not change the requirement for a DVD recorder on the instructor computer system.

## Specific Course Requirements

This section describes the specific lab requirements for each course in the SIA Curriculum.

### *The "Principles of Survivability and Information Assurance" Course*

**Hardware Requirements**

- One instructor workstation computer system with:
  - 3Ghz CPU
  - 2 GB of RAM
  - 160 GB of hard disk
  - floppy disk drive
  - CD/DVD recorder
  - 10/100 Ethernet network interface card
- One student computer system per student with:
  - 3Ghz CPU
  - 2 GB of RAM
  - 80 GB of hard disk
  - floppy disk drive
  - CD/DVD reader
  - 10/100 Ethernet network interface card
- One or more laser printers

All of these computer systems and printers can be connected together on a flat network that requires no network infrastructure components. Institutions can use hubs and switches and can even connect all of the aforementioned components together using WiFi technology if they so choose. The key is that they are all connected together.

[5] This assumes the licensing/use conditions of the software packages allow this.
[6] This assumes the licensing/use conditions of the software packages allow this.

**Software Requirements**[7]

- Red Hat LINUX Version 9
  - Distribution
    - ftp://ftp.redhat.com/pub/redhat/linux/9/en/iso/i386/shrike-i386-disc1.iso
    - ftp://ftp.redhat.com/pub/redhat/linux/9/en/iso/i386/shrike-i386-disc2.iso
    - ftp://ftp.redhat.com/pub/redhat/linux/9/en/iso/i386/shrike-i386-disc3.iso
  - Patches
    - Standard: ftp://updates.redhat.com/9/en/os/
    - Legacy: http://download.fedoralegacy.org/redhat/9/updates/i386
  - Installation
    - Red Hat LINUX Version 9 is to be installed on all instructor and student computer systems and all relevant patches applied.
- Webmin – A Web-based interface for system administration
  - Distribution
    - http://prdownloads.sourceforge.net/webadmin/webmin-1.230-1.noarch.rpm
  - Installation
    - Webmin is to be installed on all instructor and student computer systems.
- VMware Workstation 4.5.2 for LINUX
  - Distribution
    - http://www.vmware.com/download/workstation.html
  - Installation
    - One licensed copy per instructor and student computer system
- The **Supplemental Lab Materials**
  - Distribution
    - Available as part of the SIA Curriculum Reference Implementation
  - Installation
    - The *SIA-1* directory on the Supplemental Lab Materials is to be installed on all instructor and student computer systems.

**Documentation**

- Guided Tour P-LAB-01: *"Building the Lab Computer Systems for "Principles of Survivability and Information Assurance""*

[7] URLs valid as of October 2005

 

## *The "Information Assurance Networking Fundamentals" Course*

### Hardware Requirements

The hardware requirements for the lab for the "Information Assurance Networking Fundamentals" course are identical to those for the "Principles of Survivability and Information Assurance" course.

### Software Requirements[8]

- The Ethereal Network Protocol Analyzer
  - Distribution
    - http://www.ethereal.com/download.html
  - Installation
    - Ethereal is to be installed on all instructor and student computer systems.
- The Java Run Time Environment
  - Distribution
    - http://java.sun.com/j2se/1.5.0/download.jsp
  - Installation
    - The Java Run Time Environment is to be installed on all instructor and student computer systems.
- NMAP – The Network Mapper
  - Distribution
    - http://www.insecure.org/nmap/nmap_download.html
  - Installation
    - NMAP is to be installed on all instructor and student computer systems.
- Netcat networking utility
  - Distribution
    - http://netcat.sourceforge.net/download.php
  - Installation
    - Netcat is to be installed on all instructor and student computer systems.
- The Libnet Packet Construction Library
  - Distribution
    - http://www.packetfactory.net/libnet/dist/libnet.tar.gz
  - Installation
    - Libnet is to be installed on all instructor and student computer systems

[8] URLs valid as of October 2005

- The Netwox Network Toolbox
  - Distribution
    - http://www.laurentconstantin.com/en/netw/#download
  - Installation
    - Netwox is to be installed on all instructor and student computer systems.
- The **Supplemental Lab Materials**
  - Distribution
    - Available as part of the SIA Curriculum Reference Implementation
  - Installation
    - The *SIA-2* directory on the Supplemental Lab Materials is to be installed on all instructor and student computer systems.
- The Honeynet Project network captures
  - Distribution
    - http://www.honeynet.org/scans/scan22/snort-0718@1401.log.gz
    - http://www.honeynet.org/scans/scan23/sotm23.tar.gz
  - Installation
    - These network captures are to be installed on all instructor and student computer systems.

**Documentation**

- Guided Tour P-LAB-01: *"Building the Lab Computer Systems for "Principles of Survivability and Information Assurance""*
- Guided Tour N-LAB-01: *"Building the Lab Computer Systems for "Information Assurance Networking Fundamentals""*
- Guided Tour N-LAB-02: *"Building the Lab Prototype Guest Computer system for "Information Assurance Networking Fundamentals""*
- Guided Tour N-LAB-03: *"Building Guest Computer Systems for the Exercises in "Information Assurance Networking Fundamentals""*

## *The "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" Course*

**Hardware Requirements**

The hardware requirements for the lab for this course build on those for the "Principles of Survivability and Information Assurance" and "Information Assurance Networking Fundamentals" courses. In this course, the fourteen student computer systems minimum is required to build the enterprise. For all labs in all modules, except the last module, which deals with adding a new SFU to the enterprise, the additional hardware required is seven 10/100 Ethernet network interface cards installed as follows:

- Two are installed on the instructor computer system, making a total of three installed in that computer system

 

- Two are installed in one student computer system, making a total of three installed in that computer system
- One each in four student computer systems, making a total of two installed in each of those computer systems

The report entitled *"The Design and Operation of the Lab for the "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" Course in the SIA Curriculum"* describes and depicts where these additional five network interface cards are to be installed and the network topology for the entire lab. Please note that if the lab is configured for the "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" course, it will also work in this configuration for both the "Principles of Survivability and Information Assurance" and "Information Assurance Networking Fundamentals" courses.

If the Wireless Survivable Functional Unit described in the last module of this course is to be built rather than simply designed on paper, then the following additional hardware is required:

- Three more computer systems of the student computer system type
- One or more wireless network interface cards
- One or two wireless access points that are compatible with these wireless network interface cards
- Five additional network interface cards installed as follows:
    - One each in the Logging, Network Intrusion Detection Functional Unit servers
    - One for the new computer system that acts as a router/firewall connecting the Wireless network to the VPN network
    - Three in one of the new computer systems that acts as a router/firewall connecting the existing enterprise network, the VPN network, and the RADIUS network

**Software Requirements**

The software requirements for this course are not as firm as they are for the "Principles of Survivability and Information Assurance" and "Information Assurance Networking Fundamentals" courses. See the report entitled *"The Design and Operation of the Lab for the "Sustaining, Improving, and Building Survivable Functional Units (SFUs)""* for a suggested set of software for the enterprise network.

**Documentation**

Again see the report entitled *"The Design and Operation of the Lab for the "Sustaining, Improving, and Building Survivable Functional Units (SFUs)"" f*or the complete specification and the suggested network topology for this Wireless SFU.

## Concluding Remarks

The lab used in all of the courses in the SIA Curriculum is built from commodity hardware and (currently) freely-available[9] software with the exception of VMware Workstation version 4.5.2 for LINUX which must be purchased from VMware, Inc. There are guided tours that explain how an institution should install and configure various key parts of the lab, but not all of the parts. There are several parts for which the institution is responsible and must make installation, configuration, and maintenance decisions.

[9] As of October 2005

 